INL News Release
FOR IMMEDIATE RELEASE
Nov. 8, 2010

NEWS MEDIA CONTACTS:
Ethan Huffman, 208-526-0660, ethan.huffman@inl.gov
Misty Benjamin, 208-526-5940, misty.benjamin@inl.gov

Industrial Control Systems Cyber Emergency Response Team celebrates first anniversary

WASHINGTON, D.C. — The U.S. Department of Homeland Security (DHS) today recognized the first anniversary of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). The team's main operations center is based at Idaho National Laboratory.

Established in November 2009, the ICS-CERT provides the U.S. government and private industry with cyber incident response and analysis capabilities for threats affecting industrial control systems operating critical infrastructures and key resources. The DHS has 18 recognized critical infrastructure sectors and key resource sectors including the electric power grid, public health institutions, chemical manufacturing facilities and the transportation sector, among others.

During the first year of operation, the ICS-CERT:
- Collaborated with Siemens, Microsoft, Symantec and other industry partners to facilitate analysis and response to the Stuxnet worm and other malicious threats.
- Deployed fly-away teams for on-site incident response at 13 Industrial Control Systems organizations.
- Conducted malware analysis to evaluate the impacts of exploits in control systems environments.
- Coordinated incident response and mitigation activities with control systems vendors and users.
- Performed digital media analysis on items of interest to the control systems community.
- Developed technical analysis reports and distributed them to appropriate stakeholders.

"Protecting the nation's critical infrastructure systems and key resources from cyber threats is a top priority for the DHS," said Rick Lichtenfels, acting director of the DHS Control Systems Security Program. "We're proud of the contributions that the ICS-CERT has made in their first year, and look forward to building increased public-private sector partnerships."

The ICS-CERT serves as a key component of the National Cybersecurity and Communications Integration Center (NCCIC), which coordinates all cyber incident response efforts for the U.S. on behalf of DHS. For more information on DHS's control systems security efforts, please visit www.us-cert.gov/control_systems.

INL is one of the DOE's 10 multiprogram national laboratories. The laboratory performs work in each of DOE's strategic goal areas: energy, national security, science and environment. INL is the nation's leading center for nuclear energy research and development. Day-to-day management and operation of the laboratory is the responsibility of Battelle Energy Alliance.

Subscribe to RSS feeds for INL news and feature stories at www.inl.gov. Follow @INL on Twitter or visit our Facebook page at www.facebook.com/IdahoNationalLaboratory.

—INL-10-031—

News Release Archive